International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Secure Data Management in Smart Meter as an Application of IoT

Fariha Khan[1], Aruna Gawade[2]

[1]Student, Computer Engineering Department, D. J. Sanghvi College of Engineering, Mumbai, India

[2]Professor, Computer Engineering Department, D. J. Sanghvi College of Engineering, Mumbai, India

Abstract: ***The Internet of Things(IoT) is evolving rapidly and hence it becomes a necessity to understand the security challenges that can be faced by the IoT network and devices. The IoT devices are called Smart Objects which are the fundamental blocks of IoT architecture. There are many applications of IoT which include Smart City, Smart Traffic Management, Smart Waste Management, Environmental Monitoring, Smart Meter, etc. This paper discusses one such application called Smart Meter which is an essential block of Smart Grid and the security issues involved in it and the possible methods to overcome it. The security attacks to a Smart Meter can be performed by the premise owner, the utility service provider or an outsider. Usually, the attack happens on the Smart Meter itself or the information/data transmitted by the Smart Meter. This paper presents countermeasures for some of the security vulnerabilities. Rabin encryption crypto-system is proposed to secure the data transmitted between the Smart Meter and the Utility Company.***

Keywords: Smart Meter, Smart Grid, security, Internet of Things(IoT), encryption, decryption

1. Introduction

The use of sensors and Smart Objects is growing tremendously thanks to the growing advances in the field of IoT. A smart object, also known as an embedded device, thing, or sensor, is a physical element with the capability to be identifiable, and optionally it can be also able to communicate, sense, and interact with the environment and other smart objects [5]. In spite [9] of the technological advancements in IoT, the Smart Objects are still resource-constrained devices. Smart electric meter is an important block of Smart Grid. The Smart Meter is nothing but an advanced energy meter which collects information from the end user's load devices and measures the energy usage of the consumers and further sends the collected information to the utility company for better monitoring and billing. Smart meter also measures voltage and frequency and records the energy consumption of the users. Smart meter [6] supports bidirectional communications between the meter and the central system. Also, smart meter has the built-in ability to disconnect-reconnect certain loads remotely and can be used to monitor and control the user's devices and appliances to manage demands and loads within the "smart-buildings" in the future. Several sensors and control devices, supported by dedicated communication infrastructure, are utilized in a smart meter.

A Smart Meter usually collects load readings from various appliances in the user's premise. A smart meter performs four basic functions with respect to power management which include the monitoring and recording of demand, the logging of power relevant events, e.g., outages, the delivery of usage and logging information to the upstream utilities, delivering and receiving of control messages, e.g., controlling smart appliances, remote disconnect, etc [8].

It then sends the meter readings to the collector which collects data and/or information from multiple Smart Meters and forwards it to the Utility Data Centre for calculation of billing information.

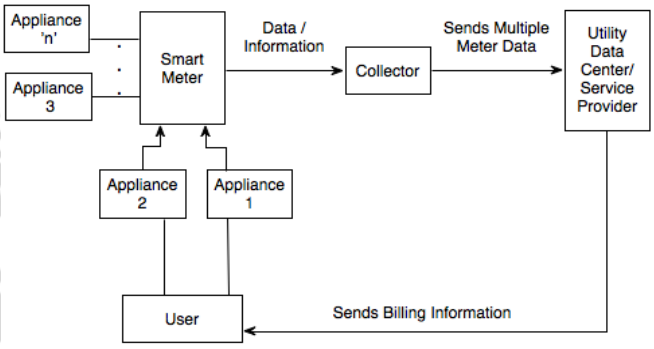

Figure 1: Smart Meter data management

The Utility Company sends the calculated bill to the user who in turn can manage his energy consumption.

The traditional electric meter would only perform recording of consumer's energy usage whereas the smart meter can collect information about a user's energy consumption, data about home devices, transfer the data to utility companies for better monitoring and billing and sometimes also smart meter to the various security attacks that are plaguing the computer network [7]. The Smart Meter communicates information between the user and the utility which makes it vulnerable to various security attacks which includes malicious codes being injected in the Smart Meter, Man In The Middle attack, Replay attack, Denial Of Service attack, Spoofing, Fake user/Impersonation, tampering, stealing, etc.

This paper focuses on few such attacks and their countermeasures depicted on the Smart Meter application.

2. Related Work

Ahmad W. Atamli, Andrew Martin [1] have briefly explained the Internet Of Things from use-cases perspective.

The use-cases that have been discussed include Power Management, Smart Car, Smart Healthcare System. They have also briefly discussed threat models which involves sources of threats, classes of attack vectors and also what possible impacts can happen on various smart objects.

Kyoungsub Song,Dongwon Seo, Haemin Park, Heejo Lee, Adrian Perrig [2] propose a novel attestation scheme, termed One-way Memory Attestation Protocol (OMAP). OMAP not only detects local attacks by constructing a checksum using a random memory traversal, but also prevents from network attacks because its response (e.g., checksum) for the attestation is forwarded in one direction from a smart meter to a utility. That is, a smart meter using OMAP generates a checksum by randomly selecting specific ranges of a memory, and forwards the checksum to a utility. Because the utility decides how the smart meter generates the checksum, the utility can verify if the memory of the smart meter is modified. This protocol was designed to overcome the drawbacks of challenge-response protocol which was easily affected by Man In The Middle attack.

Obaid Ur-Rehman, Natasa Zivic, Christoph Ruland [3] discussed the privacy and security aspects of smart metering. The potential security and privacy concerns are identified. The possible attacks on smart meters and the smart metering infrastructure are discussed and some solutions are outlined. The gateway based approach for smart metering systems and the security issues thereof are discussed.

Zubair A. Baig and Abdul-Raoof Amoudi [4] through their paper, attempt to categorize various attack types and countermeasures that exist against the Smart Grid. The paper focuses on various types of attacks that happen at different layers and their possible countermeasures.

3. Proposed System

This papers discusses some mechanisms to overcome the security and privacy breach which can happen on both, the Smart Meter as well as the crucial data/information being transmitted between the Smart Meter and the Utility Company/Service Provider.

3.1. To prevent attack on the information being transferred between Smart Meter and the Utility Company which is usually private information about a user's energy consumption, the following solution is proposed.

Rabin encryption crypto-system can be implemented to confirm that the correct message has been sent by the Smart Meter indicating the data is safe from attacks. The scheme can be explained as follows.

Step 1: Key Generation
At Utility, a public key for encryption is generated and a private key for decryption is generated respectively.
1.Two distict random prime numbers, x and y, are generated.
2. n=x*y, is computed.
3. Here, n is the public key and (x,y) are private keys.

Step 2: Encryption
Smart Meter receives the public key i.e. n from Utility Company and encrypts message M for Utility Company.
1.The message expresses the plaintext as number.
2. The text computes the value

$$C \equiv m^2 mod n, c \in N$$

3.It sends C to Utility Company

Step 3: Decryption
Utility Company receives C from Smart Meter.
1.Four messages recover the plain texts, i.e. m1, m2, m3 and m4, then

$$m_i^2 \equiv cmodn, i1,4$$

is computed.
2. The plaintext is distinguished from four messages.
3.The original message recovers m.

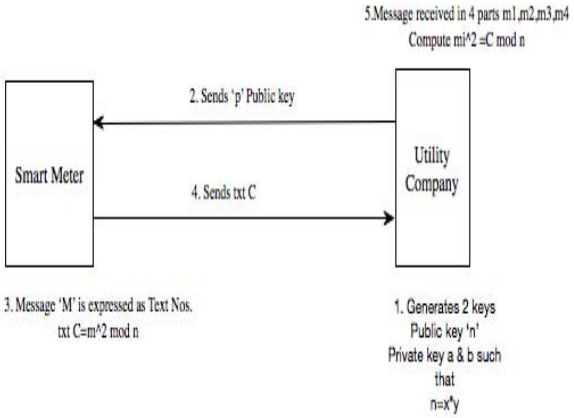

Figure 2: Rabin-encryption crypto-system

By implementing this algorithm, it can be ensured that data is transferred between the Smart Meter and the Utility Company in a secured way. This also makes sure that information being sent by the Smart Meter is not tampered or changed as the public key is known only to the Smart Meter.

3.2. Smart Meter tampering is not so uncommon. An attacker might hack the Smart Meter and pass on inaccurate reading to the Utility Company. Here, the attacker can be the owner itself who hacks the Smart Meter to generate low bill or the attacker can be an outsider who wants to take revenge with the owner and sends wrong readings to generate high electricity bill. Smart Meter hacks are very harmful as it gives idea to the attacker about the consumer's lifestyle such as which luxury electronics are present in the user's home. Also, continuous monitoring of Smart Meter by an attacker will help the attacker to know when the user is at home and when he is not depending on the load readings generated by the electrical equipments.

A solution to Smart Meter tampering is discussed below.
1) A sensor must be installed at the Smart Meter which will measure the current, voltage and other parameters at regular intervals.
2) Threshold is set for each parameter. (Threshold is set based on the user's energy consumption over a period of time).
3) If the parameter reading goes beyond the threshold, an alarm is generated and Utility Company is alerted.

The above technique will generate an alarm whenever there is very high or very low power consumption. It might happen that high power consumption by the user is a result of some public function such as parties or festivities held at the owner's premise. The Utility Company will inform the owner about their excess energy usage who in turn can try to lower their consumption of power. Thus, this technique helps the user's to keep a track of their energy usage and hence limit their consumption.

4. Conclusion

With so much developments in the field of IoT, comes many security issues. Smart Meter is a well known application of Internet of Things which will be implemented in most countries in the near future. It has various advantages over the traditional electric meter but at the same time it is vulnerable to many security and privacy breaches. In this paper, we have discussed few threats that might occur on the Smart Meter. This paper also proposes the Rabin encryption crypto-system for secure communication between Smart Meter and Utility Center which will prevent such security breaches. Also, we have discussed a simple security mechanism which is easy to implement and which informs about Smart Meter tampering to the Utility immediately allowing the Utility to take the required action.

References

[1] Ahmad W. Atamli, Andrew Martin, "Threat-based Security Analysis for the Internet of Things." 2014 International Workshop on Secure Internet of Things.
[2] Kyoungsub Song, Dongwon Seo, Haemin Park, Heejo Lee, Adrian Perrig, "OMAP: One-way Memory Attestation Protocol for Smart Meters." Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops, IEEE 2011.
[3] Obaid Ur-Rehman, Natasa Zivic, Christoph Ruland, "Security Issues in Smart Metering Systems."
[4] Zubair A. Baig and Abdul-Raoof Amoudi, "An Analysis of Smart Grid Attacks and Countermeasures." Journal of Communications Vol. 8, No. 8, August 2013.
[5] Antonio J. Jara, Yann Bocchi, Dominique Genoud, "Social Internet of Things: The potential of the Internet of Things for defining human behaviours." 2014 International Conference on Intelligent Networking and Collaborative Systems.
[6] Jixuan Zheng, David Wenzhong Gao, Li Lin, "Smart Meters in Smart Grid: An Overview." 2013 IEEE Green Technologies Conference.
[7] Salman Yussof, Mohd. Ezanee Rusli, Yunus Yusoff, Roslan Ismail, Azimah Abdul Ghapar, "Financial Impacts of Smart Meter Security and Privacy Breach," 2014 International Conference on Information Technology and Multimedia (ICIMU), November 18 – 20, 2014, Putrajaya, Malaysia.
[8] Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel, "Energy Theft in the Advanced Metering Infrastructure."
[9] Alexandros Fragkiadakis, Pavlos Charalampidis, and Elias Tragos, "Adaptive compressive sensing for energy efficient smart objects in IoT applications."